Distinguishing Maximal Orders of Quaternion Algebras by their Short Elements

Ilya Chevyrev and Steven Galbraith

University of Auckland, New Zealand



Summer School, Nelson, NZ, January 2015

11-16 January 2015
Nelson, South Island, NZ

Speakers: Pierre Deligne, Gus Lehrer, Cheryl Praeger, René Schoof, Richard Weiss.

Auckland, New Zealand, December 2015

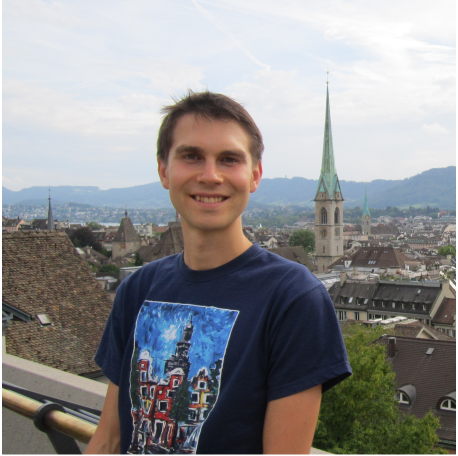
Plan

- Background and some of my favourite questions
- Why is this talk in a session on lattices?
- Sketch of results and algorithm
- Shall we talk about something else?

Thanks: David Kohel, Drew Sutherland.

Please ask questions at any time.

Ilya Chevyrev



Elliptic Curves and Isogenies

- An **elliptic curve** over a field $\mathbb{k}$ is a non-singular projective cubic curve. The set of $\mathbb{k}$-rational points is a group.
- An **isogeny** $\phi : E_1 \to E_2$ of elliptic curves is a morphism that is a group homomorphism.
- Isogenies satisfy a degree 2 characteristic polynomial $T^2 - \mathrm{Tr}(\phi)T + \deg(\phi) = 0$, having discriminant $D = \mathrm{Tr}(\phi)^2 - 4\deg(\phi) \leq 0$.
- Tate's isogeny theorem: Let E_1, E_2 be elliptic curves over a finite field $\mathbb{F}_q$. Then $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ iff there is an isogeny $\phi : E_1 \to E_2$ over $\mathbb{F}_q$.
- $\mathrm{End}(E) = \{$isogenies $\phi : E \to E$ over $\overline{\mathbb{F}}_q\}$.
- $\mathrm{End}(E)$ is either an order in an imaginary quadratic field (ordinary) or a maximal order in a definite quaternion algebra B_p ramified at $\{p, \infty\}$ (supersingular).

Some Computational Questions

- Given E over $\mathbb{F}_q$ to compute $\mathrm{End}(E)$.
  Two cases: ordinary and supersingular.
- Given E, E' over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ to compute an isogeny from E' to E.
  Two cases: ordinary and supersingular.
- Given q, N construct an elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = N$.
- Construct an elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = N$ for pairs (q, N) with certain "desired properties".
- Given a maximal order $\mathcal{O}$ in the quaternion algebra B_p to construct an elliptic curve E over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ with $\mathrm{End}(E) \cong \mathcal{O}$.

Hilbert Class Polynomial

- Consider fundamental discriminant $D < 0$. The Hilbert class polynomial $H_D(X) \in \mathbb{Z}[X]$ has property: Given $E/\Bbbk$, if $H_D(j(E)) = 0$ then $\mathrm{End}(E)$ contains an isogeny of discriminant D.
- Specifically, the roots in $\mathbb{C}$ of $H_D(X)$ are the j-invariants of the elliptic curves over $\mathbb{C}$ possessing the quadratic order $\mathcal{O}_D = \mathbb{Z}[\frac{1}{2}(D + \sqrt{D})]$ as their endomorphism ring.
- Class polynomials are used in the CM method for constructing curves with a given group order/endomorphism structure.
- What other applications might there be?

Bröker's Algorithm

- Goal: Given $q = p^a$ to construct a supersingular curve over $\mathbb{F}_q$ with specified trace of Frobenius.
- Main idea: Choose small prime ℓ such that $(\frac{-\ell}{p}) = -1$ then find root of $H_{-\ell}(X)$ or $H_{-4\ell}(X)$ in $\mathbb{F}_q$.
- Construct corresponding E and twist if necessary.
- CM theory tells that E is supersingular, as p is inert in $\mathbb{Q}(\sqrt{-\ell})$.

Idea

- Problem: Given a maximal order $\mathcal{O}$ construct E such that $\mathrm{End}(E) \cong \mathcal{O}$.
- A simple idea is to find some elements in $\mathcal{O}$ of small discriminant $D_1, D_2, \cdots$ and take

$$G(X) = \gcd(H_{D_1}(X), H_{D_2}(X), \cdots).$$

- Then hope that $\deg(G) \leq 2$ and that taking roots gives $j(E)$ and hence E.
- Related application: Can we determine $\mathrm{End}(E)$ by testing if $H_D(j(E)) = 0$ for various discriminants D?
- **Question:** Is a maximal order $\mathcal{O}$ in quaternion algebra B_p determined by a small number of discriminants.

Lattices and Ternary Forms

- Consider the $\mathbb{Z}$-module $\mathcal{O}^T = \{2x - \mathrm{Tr}(x) : x \in \mathcal{O}\}$ of rank 3.
- Note that $y \in \mathcal{O}^T$ implies $\mathrm{Tr}(y) = 0$ (pure quaternion).
- The reduced norm on $\mathcal{O}$ is a ternary quadratic form Q, making $\mathcal{O}^T$ a lattice.
- The volume of the lattice is $4p^2$.
- Let $\mathcal{O}'$ be another maximal order in the same quaternion algebra B_p and let Q' be the ternary form of $\mathcal{O}'^T$.
  If Q' is equivalent to Q, in the sense of quadratic forms, then is $\mathcal{O}'$ isomorphic to $\mathcal{O}$ ($\mathcal{O}' = c\mathcal{O}c^{-1}$ for some $c \in B_p$)?
- **Theorem:** (Schiemann) Ternary quadratic forms are determined up to equivalence by their theta series.
- We will show that one can check equivalence by only checking a very small number of coefficients of the theta series.

Bulguksa Lattices

Main Theorems

Theorem

Let $\mathcal{O}$ and $\mathcal{O}'$ be two maximal orders of B_p. Let $\mathcal{O}^T$ and $\mathcal{O}'^T$ have the same successive minima $D_1 \leq D_2 \leq D_3$. Assume moreover that $D_1 D_2 < 16p/3$ and that p is sufficiently large. Then $\mathcal{O}$ and $\mathcal{O}'$ are of the same type (= isomorphic).

Theorem

Let $p > 286$ and $\mathcal{O}$, $\mathcal{O}'$ be two maximal orders of B_p. Let D_1, D_2 and D_3 be the successive minima of $\mathcal{O}^T$ and let $x, y \in \mathcal{O}^T$ be such that $Nr(x) = D_1$ and $Nr(y) = D_2$. Suppose that $D_1 D_2 < \frac{16}{3} p$ and that D_1, D_2, $Nr(x+y)$, $Nr(x-y)$ and D_3 are all "represented optimally" in $\mathcal{O}'^T$ and that $\theta'_{\mathcal{O}^T}(D_3) \leq \theta'_{\mathcal{O}'^T}(D_3)$. Then $\mathcal{O}$ and $\mathcal{O}'$ are of the same type.

The condition $D_1 D_2 < 16p/3$

Lemma

Let $\mathcal{O}$ be a maximal order in B_p that contains an element π such that $\pi^2 = -p$ (and hence $j(\mathcal{O}) \in \mathbb{F}_p$). Then $D_1 D_2 < 16p/3$.

Proof based on a paper of Kaneko.

Elkies showed $D_1 \leq 2p^{2/3}$ for any maximal order in B_p and Yang has shown that this is best possible.

Method of Proof

- Let $x, y \in \mathcal{O}^T$ have norms D_1 and D_2 respectively. Similarly $x', y' \in \mathcal{O}'^T$.
- Prove that $\langle x, y \rangle$ and $\langle x', y' \rangle$ isometric, using $4D_1D_2 - \mathrm{Tr}(x\overline{y})^2 \equiv 0 \pmod{p}$ and simple geometry of numbers.
- **Lemma:** $w = 2xy - \mathrm{Tr}(xy) \in \mathcal{O}^T \cap \langle x, y \rangle^{\perp}$.
- More geometry of numbers completes the result.
- Proof of Theorem 2 requires further arguments to reduce to case of Theorem 1.
- Everyone agrees there should be a nicer proof.

Algorithm to Construct E

- Let $\mathcal{O}$ be a maximal order in B_p given as a $\mathbb{Z}$-basis.
- Use lattice algorithms to find several small norms $d_1, d_2, \ldots, d_n$ of "primitive" elements in $\mathcal{O}^T$.
- Hence $(X - j(E))$ is a factor of $\gcd(H_{-d_1}(X), H_{-d_2}(X), \ldots, H_{-d_n}(X))$.
- Take multiple roots into account.
- When $j(E) \in \mathbb{F}_p$ then our theorems imply the algorithm terminates with a degree 1 polynomial.
- In this case, all d_i are such that $|d_i| = O(p)$.
- Computing $H_d(X)$ can be done in time $\tilde{O}(|d|)$ by Belding-Bröker-Enge-Lauter or Sutherland.
  This is the limiting step, as poly degree is $O(|d|^{0.5+\epsilon})$.
- So overall complexity $\tilde{O}(p)$.
- Examples in paper.

Algorithm when $j(E) \notin \mathbb{F}_p$

- Conjecture that the algorithm terminates with degree two polynomial.
- Conjecture that running time is still $\tilde{O}(p)$.
- Can consider an algorithm to match $\{\mathcal{O}\}$ with the set $\{j(E)\}$ over all supersingular curves.
- Cerviño proposed such an algorithm.
  As far as we can tell, his algorithm requires $O(p^{3+\varepsilon})$ field operations.
- Our method has the improved complexity $O(p^{2.5+\varepsilon})$ field operations.
- Our algorithm is always guaranteed to halt!
- For subcase of $j(E) \in \mathbb{F}_p$, Cerviño needs $O(p^{2.5+\varepsilon})$ and we need $O(p^{1.5+\varepsilon})$.

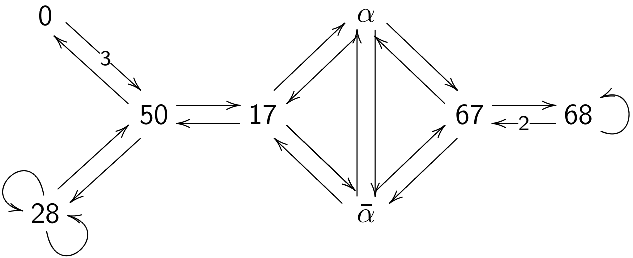
Kohel-Lauter-Petit-Tignol

The last talk of the conference has tools that should lead to better solutions to these problems.

Computing Isogenies between Supersingular Elliptic Curves over $\mathbb{F}_p$

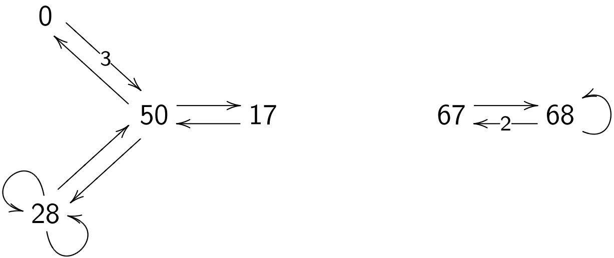
- Joint work with Christina Delfs.
- Problem is to find sequence of isogenies between two given supersingular elliptic curves.
- The number of supersingular elliptic curves in $\overline{\mathbb{F}}_p$ is approximately $p/12$, but there are only $p^{0.5+\epsilon}$ supersingular elliptic curves over $\mathbb{F}_p$.
- So finding a path between two supersingular elliptic curves over $\mathbb{F}_p$ should be easier than the general problem.
- Can reduce general case to this case using random walks.
- We solve the sub-problem using CM theory and algorithm from S. Galbraith, F. Hess, N. P. Smart, "Extending the GHS Weil descent attack", EUROCRYPT 2002.

Full supersingular isogeny graph



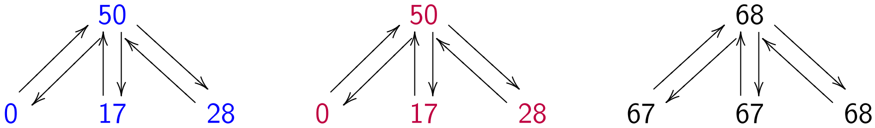
Supersingular Isogeny Graph $X(\overline{\mathbb{F}}_{83}, 2)$

Subgraph



Subgraph consisting $j \in \mathbb{F}_{83}$

New graph

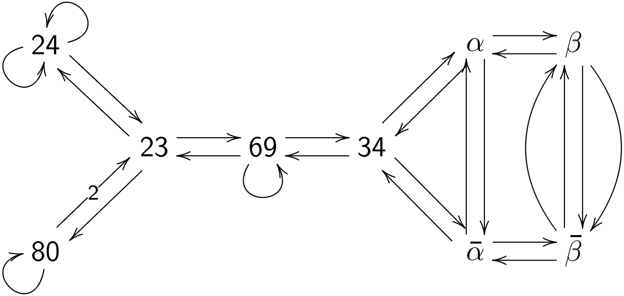


$X(\mathbb{F}_{83}, 2)$

Structure theorem ($p > 3$ prime)

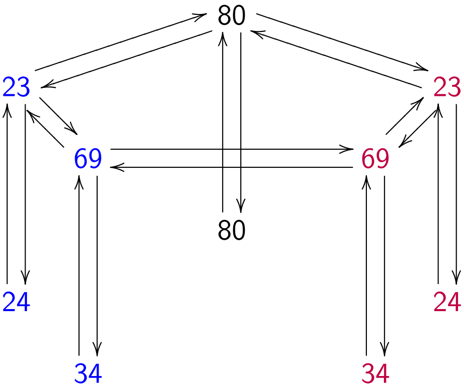
1. $p \equiv 1 \pmod 4$: There are $h(-4p)$ $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, all having the same endomorphism ring $\mathbb{Z}[\sqrt{-p}]$. From every one there is one outgoing $\mathbb{F}_p$-rational horizontal 2-isogeny as well as two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.
2. $p \equiv 3 \pmod 4$: There are two levels in the supersingular isogeny graph. From each vertex there are two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.
   - 2.1 If $p \equiv 7 \pmod 8$, on each level $h(-p)$ vertices are situated. Surface and floor are connected 1:1 with 2-isogenies and on the surface we also have two horizontal 2-isogenies from each vertex.
   - 2.2 If $p \equiv 3 \pmod 8$, we have $h(-p)$ vertices on the surface and $3h(-p)$ on the floor. Surface and floor are connected 1:3 with 2-isogenies, and there are no horizontal 2-isogenies.

Example 2: $p = 103 \equiv 7 \pmod 8$



Supersingular Isogeny Graph $X(\overline{\mathbb{F}}_{103}, 2)$

New



$X(\mathbb{F}_{103}, 2)$

Thank You